IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
5:19-CV-215-BO

RICKEY KIMBRIEL and PAULA KIMBRIEL, individually, and on behalf of all others similarly situated, Plaintiffs, v. ABB, INC., and BALDOR ELECTRIC COMPANY n/k/a ABB MOTORS AND MECHANICAL, INC., Defendants.	)	ORDER

This matter is before the Court on defendants' motion to dismiss plaintiffs' complaint. [DE 15]. Plaintiffs have responded and the motion is now ripe for disposition. Plaintiffs have also filed a consent motion [DE 22] for leave to file excess pages. For the reasons that follow, defendants' motion to dismiss [DE 15] is GRANTED and plaintiffs' complaint is DISMISSED. The consent motion [DE 22] is DENIED.

BACKGROUND

Plaintiff Rickey Kimbriel has been a machine operator at defendant Baldor Electric Company ("Baldor") since 2015. DE 1, ¶ 20. Baldor is a subsidiary of defendant ABB, Inc., an industrial technology company incorporated in Delaware with its principal place of business in Cary, North Carolina. *Id.* ¶¶ 14, 21. Rickey and his wife, Paula Kimbriel, have participated in ABB's health benefits plan ("the Plan") since Rickey joined the company. *Id.* ¶ 12. When joining the Plan, Ricky and Paula provided sensitive personal data, including full legal names, addresses, birth dates, and social security numbers, which were stored in the Plan's database along with other

information such as their plan member ID, and were accessible through certain ABB employee email accounts. *Id.* ¶¶ 25–27. ABB also had Rickey's checking account information for purposes of direct deposit. *Id.* ¶ 24.

On or about August 25, 2017, certain ABB employees' emails were hacked through a phishing scheme, resulting in the compromise of personally identifiable information ("PII") associated with the Plan. *Id.* ¶¶ 28–29, Ex. A. Rickey was first notified of the hack at an employee meeting at the end of August 2017. *Id.* ¶ 28. On September 7, 2017, ABB sent out a formal notice informing affected employees of the hack, stating that Rickey and his dependent's sensitive PII associated with the plan, specifically names, addresses, plan member IDs, birth dates, and social security numbers, may have been exposed. *Id.* ABB represented it would pay for identity monitoring services and encouraged affected employees to take additional cautionary steps, including placing a fraud alert with the Federal Trade Commission and a security freeze on their credit files. *Id.* ¶ 40. The PII of the Plan's 17,996 participants was compromised by the breach. *Id.* ¶ 5.

In response to the security breach, Rickey Kimbriel stopped making 401(k) contributions, resulting in additional taxes that would have otherwise been deferred. *Id.* ¶ 41. On February 13, 2019, a credit-monitoring service notified Paula Kimbriel of five unauthorized credit inquiries with banking institutions in four different states. *Id.* ¶ 42.

Plaintiffs Rickey and Paula Kimbriel bring this putative class action on behalf of all the nearly 18,000 victims of the ABB security breach. They assert seven[1] claims for relief. They allege that defendants' data security practices and disclosures to employees after the breach violated the North Carolina Unfair & Deceptive Trade Practices Act, N.C. Gen. Stat § 75-1.1. *Id.* ¶¶60–70.

[1] Plaintiffs' complaint skips Count V, and so the Court counts seven, not eight, causes of action.

They allege defendants' breached a fiduciary duty by not properly safeguarding the information. *Id.* ¶¶71–76. They further allege additional claims under negligence, negligence per se, bailment, breach of contract, and breach of implied contract. *Id.* ¶¶77–90; 91–97; 98–103; 104–07; 108–18.

Defendants have moved to dismiss all of plaintiffs' causes of action under both Rule 12(b)(1) and Rule 12(b)(6) of the Federal Rules of Civil Procedure. [DE 15]. Defendants argue plaintiffs lack standing under Article III to bring this action because they have not alleged injury-in-fact. Defendants also argue that, even if plaintiffs do have standing to pursue their claims, they fail to state a claim on which relief can be granted.

DISCUSSION

Defendants' motion to dismiss

Defendants have moved to dismiss plaintiffs' complaint for lack of subject-matter jurisdiction under Rule 12(b)(1). "Subject-matter jurisdiction cannot be forfeited or waived and should be considered when fairly in doubt." *Ashcroft v. Iqbal*, 556 U.S. 662, 671 (2009) (citation omitted). "Article III of the Constitution limits federal courts' jurisdiction to certain 'Cases' and 'Controversies.'" *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 408 (2013). "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." *Id.* (internal quotations omitted). In a class action, the Court "analyze[s] standing based on the allegations of personal injury made by the named plaintiffs." *Beck v. McDonald*, 848 F.3d 262, 269 (4th Cir. 2017). To establish standing, plaintiffs must show they have suffered an injury-in-fact—an injury that is "concrete, particularized, and actual or imminent[.]" *Clapper*, 568 U.S. at 409. The injury-in-fact must be "fairly traceable to the challenged action[,] and redressable by a favorable ruling." *Id.* Threatened injuries cannot be speculative, but "must be certainly impending." *Id.*

Plaintiffs claim the following injuries or threatened injuries: (1) loss of opportunity to control their PII; (2) diminution of the value of their PII; (3) compromise/publication of their PII; (4) out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud; (5) Opportunity cost—lost wages and productivity—associated with their efforts to address and mitigate actual and future consequences of the breach; (6) delay in receipt of tax monies; (7) unauthorized use of stolen PII; (8) continued risk to their PII; and (9) current and future costs of time, money, and effort. DE 1, ¶ 45. They also make a general assertion of "monetary losses, lost time, anxiety and emotional distress." *Id.*

Plaintiffs' complaint must be dismissed because this Court lacks subject-matter jurisdiction over plaintiffs' claims. Despite their list, plaintiffs' have not alleged that they have suffered a concrete injury, or that one is certainly impending, because they fail to allege a sufficient factual basis from which to conclude that their hacked PII has actually been used, or will be used, in identity theft or fraud.

This case sits between two recent decisions, *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) and *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018), both of which address injury-in-fact in the data privacy context. *Beck* was a consolidated appeal of two cases involving data breaches at the Williams Jennings Bryan Dorn Veterans Affairs Medical Center. 848 F.3d at 266. The cases involved compromised PII from a computer and boxes of pathology reports that were either lost or stolen. *Id.* at 267–68. The plaintiffs' asserted injuries were "increased risk of future identity theft" and "costs of protecting against" identity theft. *Id.* at 273. The court held that the plaintiffs did not have standing because, critically, they could neither show that their data was actually used nor allege enough plausible facts to show that threatened future harms were "certainly impending." *Id.* at 275. In contrast, the plaintiffs in *Hutton* were

victims of credit card fraud after their personal information was stolen in a data breach of the National Board of Examiners in Optometry ("NBEO"). 892 F.3d at 616–17. The court interpreted *Beck* as emphasizing that the "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Id.* at 621. But the *Hutton* plaintiffs had suffered an injury-in-fact because their data had actually been used to open fraudulent credit card accounts. *Id.* at 622.

Here, plaintiffs' only factual allegation suggesting that their stolen PII has actually been used, or is likely to be used, is the credit inquiries in 2019. By plaintiffs' own admission, the credit inquiries do not, by themselves, constitute an independent injury-in-fact. DE 23 at 8. Instead, the question is whether the credit inquiries, coupled with the fact that the breach was a result of an allegedly targeted phishing scheme, constitute a sufficient factual basis to conclude there is a certainly impending risk of identity theft.

Plaintiffs present a stronger case than the plaintiffs in *Beck*, but ultimately, their asserted injuries are still too speculative to meet the "certainly impending" threshold. Nothing in the complaint connects the credit inquiries to the hack at ABB, which occurred eighteen months earlier. And while *Beck* explained that a targeted hack supports a finding of injury-in-fact because it is indicative of the hacker's intent to use the PII, it did not hold that a targeted hack was a dispositive or even an overriding factor. Plaintiffs are 2 of 17,996 participants affected by the ABB data breach. Without more, the credit inquiries do not provide enough of a factual basis to plausibly show that plaintiffs' compromised data is being used or that future use of the data is "certainly impending." The connection between the credit inquiries and the data breach, like plaintiffs' asserted injuries, is too speculative.

Accordingly, the Court addresses the plaintiffs' nine asserted injuries.

Plaintiffs' first three asserted injuries (loss of control, diminution in value, and compromise, publication and/or theft of PII) cannot constitute injury-in-fact. All victims of security breaches suffer loss of control of their PII, a diminution of its value if and when the PII is sold on the black market, and a compromise of their PII. Were it the case that these harms constituted injury-in-fact, all victims of data breaches would satisfy the injury requirement. But this is foreclosed by precedent. *See Hutton*, 892 F.3d 621 ("[*Beck*] emphasized that a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft."). *Beck* also forecloses plaintiffs' general claim of anxiety and emotional distress as a basis for Article III standing. 848 F.3d at 272.

Plaintiffs' fourth and fifth injures cannot satisfy the injury requirement because, although they are concrete expenditures of time and resources, they are "self-imposed harms" in response to a speculative threat. *Id.* at 276–77. Because plaintiffs have not alleged facts showing that the risk of identity theft or fraud is "certainly impending," the out-of-pocket costs and efforts to remediate and mitigate the effects of the breach cannot serve as a basis for injury-in-fact. *Id.* This also applies to any taxes paid by plaintiffs on increased taxable income as a result of discontinuing 401(k) deferrals, as well as plaintiffs' ninth asserted injury, future costs and effort to protect themselves from the breach.

Plaintiffs' remaining injuries (delayed tax refunds, unauthorized use of stolen PII, and continued risk to their PII) are purely speculative future injuries. Plaintiffs have neither alleged that their tax refunds have actually been delayed nor that their stolen data has actually been used as a result of the hack. As explained above, there is not a sufficient factual basis to connect the

2019 credit inquiries to the 2017 hack of data to push this case into the "certainly impending category." As a result, these alleged future harms are simply too speculative.

In sum, plaintiffs have failed to show an injury-in-fact. They have not alleged that they suffered a concrete injury, at least not one that was not a self-imposed harm in response to the speculative threat. Furthermore, while plaintiffs' speculation about future harms resulting from the data breach is understandable, even objectively reasonable, the complaint simply does not allege enough facts to conclude that these harms are certainly impending. Accordingly, plaintiffs' complaint must be dismissed for lack of Article III jurisdiction.

Plaintiffs' motion to exceed page limit

With the consent of defendants, plaintiffs moved to exceed the page limits set by Local Civil Rule 7.2. The Court has dismissed the case on standing grounds and is not in need of additional briefing on the merits of plaintiffs' causes of action. To the extent the additional pages would address the standing issue, the Court is not convinced it would benefit from additional briefing. Therefore, plaintiffs' motion to exceed the page limit is denied.

CONCLUSION

For the above reasons, defendants' motion to dismiss [DE 15] for lack of subject-matter jurisdiction is GRANTED and plaintiffs' complaint is DISMISSED. Plaintiffs' consent motion [DE 22] is DENIED. The Clerk is DIRECTED to close the case.

SO ORDERED, this 1 day of October, 2019.

Terrence Boyle

TERRENCE W. BOYLE
CHIEF UNITED STATES DISTRICT JUDGE